

暗号化のためのOpenSSLを使用したCMSのCSRの設定

内容

[概要](#)

[前提条件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

概要

このドキュメントでは、Open Secure Sockets Layer(OpenSSL)を使用してCisco Meeting Server(CMS)の証明書を作成する方法について説明します。

著者 : Cisco TACエンジニア、Moises Martinez

前提条件

次の項目に関する知識があることが推奨されます。

- SSLを開きます。
- CMSの設定。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアに基づいています。

- OpenSSL Light 1.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップ1:OpenSSL Light 1.1をダウンロードします。

ステップ2 : コンピュータにOpenSSLをインストールします。

ステップ3:SSLがインストールされたフォルダに移動します。通常はC:\Program Files\OpenSSL-Win64\binにインストールされます。

Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB

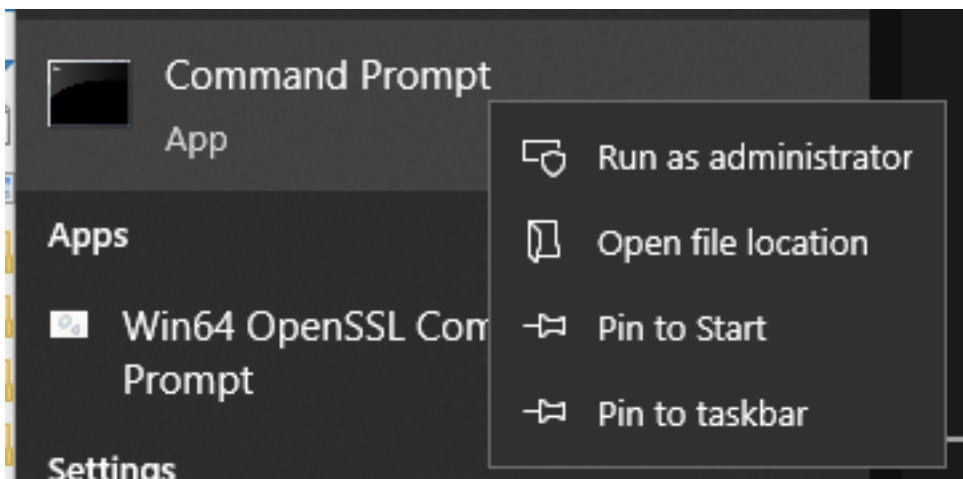
ステップ4：メモ帳を開き、次の例に示すように、証明書署名要求(CSR)に必要な情報を入力します。

```
[req] distinguished_name = req_distinguished_name req_extensions = v3_req prompt = no
[req_distinguished_name] C = US ST = California L = San Jose O = TAC OU = IT CN =
cms.tac.cisco.com [v3_req] extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt_names
[alt_names] DNS.1 = webbridge3.tac.cisco.com DNS.2 = webadmin.tac.cisco.com DNS.3 =
xmpp.tac.cisco.com
```

ステップ5:CSRの情報を入力すると、次のパスにtac.confとして保存されます。C:\Program Files\OpenSSL-Win64\bin

Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB
tac.conf	12/16/2021 5:07 PM	CONF File	1 KB

ステップ6:PCでコマンドプログラムを開き、[管理者として実行]を選択します。



ステップ7: コマンドプロンプトでファイルが保存されているパスに移動し、`openssl.exe`コマンドを入力してenterを選択します。

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe_
```

ステップ8: 次のコマンドを実行します。 `req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf`。

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf_
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
Generating a RSA private key
.....++++
writing new private key to 'cms.key'
-----
```

確認

エラーが表示されない場合、同じフォルダに2つの新しいファイルが生成されます。

- `cms.key`
- `cms.csr`

Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tac.conf	12/16/2021 5:07 PM	CONF File	1 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB
cms.csr	12/16/2021 5:25 PM	CSR File	2 KB
cms.key	12/16/2021 5:25 PM	KEY File	4 KB

この新しいファイルcms.csrは、認証局(CA)によって署名できます。